ORM PTO-1449 U.S. DEPARTMENT OF COMMER PATENT AND TRADEMARK OFFI LIST OF DOCUMENTS CITED BY APPLICANT			CE NIT-294 APPLICANT M. KAMINAGA et a	SERIA		: 1					
(Use several sheets if necessary)				y) 	FILING DATE GROUP August 29, 2001						
				U.S. PATE	NT DOCUMENTS		•				
EXAMINER INITIAL		DOCUMENT	DATE		NAME	CLASS	SUBCLASS		DATE ropriate)		
•	AA										
	АВ							T T			
	AC							8.69 3.69			
	AD							26			
	AE							100			
	AF			•			,				
	AG	,						<u>'</u>			
	АН										
	Al						·				
	AJ							·			
	AK										
			•	FOREIGN PA	TENT DOCUMENTS						
		DOCUMENT	DATE		COUNTRY	CLASS	SUBCLASS	YES	NO		
	AL	4									
	АМ										
	AN										
	АО										
	АР										
			OTHER DOCUM	MENTS (Including	Author, Title, Date, Pertiner	nt Pages, etc.)					
20	AR _	SMART	SMART CARD HANDBOOK, p. 263								
30	AS -	Tamper	Tamper Resistance - a Cautionary Note, pp. 1-11.								
	АТ	Chines	Chinese Remaindering Based Cryptosystems in the Presence of Faults,								
70											
EXAMINER	$\overline{}$	7.1-	Gay Davis		DATE CONSIDERED 0	26/05			_		

FORM PTO-1449 (REV. 7-80)			U.S. DEPARTMENT OF COMMERC PATENT AND TRADEMARK OFFICE		CE ATTY, DOCKET NO. CE NIT-294		SERIAL NO.				
					APPLICANT						
L	LIST C		S CITED BY APP		M. KAMINAGA et	al					
(Use several sheets if necessary)			eral sheets if necessary)		FILING DATE		GROUP				
				August 29, 2001							
	2			U.S. PATEN	IT DOCUMENTS	•					
• EXAMINER INITIAL		DOCUMENT	DATE		NAME	CLASS	SUBCLASS	FILING (If Appr	DATE opriate)		
-	AA										
	АВ										
	AC										
	AD										
	ΑE										
	AF					٠					
	AG				·						
	АН										
	Al	,									
	AJ										
	AK										
				FOREIGN PAT	ENT DOCUMENTS	·					
		DOCUMENT	DATE		COUNTRY	CLASS	SUBCLASS	TRANSLATION YES NO			
	AL										
	АМ		·								
	AN										
	АО										
	AP										
			OTHER DOCUME	NTS (Including)	Author, Title, Date, Pertine	ent Pages, etc.,)				
B	AR	Modular	Modular Multiplication Without Trial Division:, P. Montgomery, pp. 519-521.								
	AS					· · · · · · · · · · · · · · · · · · ·					
	1 [-			• •	<u> </u>					
ŀ	AT										
EVANUES		7			DATE CONSIDERED						
EXAMINER		7-31)_		DATE CONSIDERED	126/05					

·		OIPE		/	<i>J</i>					
		AU6-0 8 200	E SELECT OF SELE				Sheet	1	of 2	
FORM PTO	1449	TRADEN	S.S. DEPART	MENT OF COMMERCE TRADEMARK OFFICE	ATTY. DOCKET NO.	SERIAL 09/94	NO. 0 985		<u>_</u>	
		OF DOCUMEN			E NIT-294 09/940,985 APPLICANT M. KAMINAGA et al					
			sheets if necessa		FILING DATE	GROUP				
					August 29, 2001	2137	·			
				U.S. PATENT	DOCUMENTS					
* EXAMINER INITIAL		DOCUMENT	DATE		NAME	CLASS	SUBCLASS		opriate)	
	AA									
	АВ				·					
	AC			·						
	AD									
	ΑE									
	AF				· .					
	AG									
	AH.									
	Al									
	AJ									
	AK									
				FOREIGN PATE	ENT DOCUMENTS		•			
		DOCUMENT	DATE		COUNTRY	CLASS	SUBCLASS	TRANS YES	NO	
3)	AL	0946018	09/1999	EUROPE						
30		W0 00/42511	07/2000	PCT						
30	AN	WO	12/1999	PCT						
	AO	99/63696								
	AP				:					
	17.		OTHER DOCU	MENTS (Including Au	ithor, Title, Date, Pertinent P	ages, etc.)				
-30	AR	"A Tim	ing Attack ler. CHES	against RSA wi	ith the Chinese Rem 5, pp. 109-124.	ainder Th	eorem", V	Verne	<u></u>	
	AS									
	AS									
EXAMINER	2		Inchang L	Davis 1	DATE CONSIDERED	65		******	*********	
* EXAMINE with next comm	R: Initi	in to applicant.	red, whether or not cita	tion is in conformance with MPE	P 609; Draw line through citation if not in o	conformance and no	t considered. Inclu	de copy of	this form	